UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

| | |
|---|---|
| 1) American Airlines Federal Credit Union,<br>Plaintiff,<br><br>vs.<br><br>1) Sonic Corp.; 2) Sonic Industries, Inc.; 3) Sonic Capital LLC; 4) Sonic Industries LLC; 5) Sonic Franchising LLC; and 6) Sonic Restaurants, Inc.,<br>Defendants. | CLASS ACTION COMPLAINT<br><br>Case No. CIV-19-208-G<br><br><br><br>JURY TRIAL DEMANDED |

# CLASS ACTION COMPLAINT

## INTRODUCTION

1. American Airlines Federal Credit Union ("AAFCU") brings this class action lawsuit against Sonic Corporate and its subsidiaries (collectively, "Sonic"), for a data breach stemming from its unreasonable data security measures. Sonic is a nationwide fast-food restaurant, unique for its drive-in experience. In 2017, Sonic announced that its restaurants were breached by hackers who placed malware on Sonic's payment systems. The breach resulted in the theft of payment card information ("PCI") from millions of debit and credit cards used by Sonic's customers, including payment cards issued by AAFCU and used by its members at Sonic. Sonic's Data Breach rendered that payment card information worthless because members can no longer safely and reliably use that payment card information without the threat of fraud. Therefore, AAFCU and other financial institutions must reissue payment cards to their members and take immediate measures to prevent and reimburse fraudulent charges. Although Sonic has not provided any information on the length of the breach or its scope, the breach compromised an estimated five million payment cards.

2. Sonic's Data Breach resulted from the exploitation of well-known vulnerabilities in point-of-sale ("POS") systems, the systems businesses use to collect and process payment card information, and the Cardholder Data Environments, the networks that allow for the confirmation and authorization of payment information. Hackers looking to steal consumer purchasing information have targeted POS systems since at least 2005. In the last five years, malware placed on POS systems caused practically every major data breach involving retail stores or fast-food chains and resulted in millions of compromised payment cards. Data security experts have repeatedly warned, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[1]

3. Despite the known vulnerabilities of POS systems to data breaches, Sonic took inadequate steps to enhance its data security to protect its POS systems and CDE from a breach. Indeed, as discussed below, Sonic specifically chose not to implement certain industry-standard best practices such as Point-to-Point encryption, using updated software and systems and implanting endpoint detection systems that could have detected and prevented the breach.

4. The FTC has also issued guides and other resources designed to inform businesses of the best practices in data security and to encourage businesses to prioritize data security. Similarly, the Payment Card Industry Security Standards Council (Visa, American Express, Discover, JCB International, and MasterCard) requires merchants to meet certain minimum data security standards. These protections are specifically designed to empower businesses to prevent data breaches.

[1] *Point of Sale Security: Retail Data Breaches At a Glance*, Datacap Systems, Inc. (May 12, 2016), https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance#.

5. Given the highly publicized data breaches that have occurred over the past four years, Sonic fully knew its POS systems would be a target for hackers, understood the vulnerabilities of its POS systems which, if not resolved, increased the likelihood of a breach, and was aware of available, reasonable data security measures that would prevent hackers from infiltrating its systems, prevent the application of malware on its POS systems, and allow for fast identification and remediation of any intrusion. Furthermore, Sonic fully knew that a breach would cause significant harm to the financial institutions responsible for re-issuing compromised cards and reimbursing consumers for fraudulent transactions caused by a data breach.

6. Despite Sonic's knowledge of the vulnerabilities of its POS systems and the consequences of a breach, it completely failed to prioritize its data security. In September 2017, Sonic first admitted that it discovered that hackers had infiltrated POS systems at its restaurants and, for an undisclosed amount of time, stole customer payment information. Sonic completely failed to discover the hackers or recognize that it had been breached, and only learned that its systems were compromised after being informed that card brands were alerting payment card issuers of potential fraudulent activity on credit and debit cards used at Sonic's restaurants. By the time Sonic discovered the breach, hackers had compromised millions of payment cards. The large number of cards compromised due to Sonic's breach indicates the breach likely lasted for several months. Although Sonic has never publicly provided the breach's exposure window, a settlement agreement entered into between

Sonic and a class of consumer plaintiffs who sued Sonic for the data breach indicates the Data Breach began on April 7, 2017 and lasted until October 28, 2017.[2]

7. Sonic's Data Breach was the inevitable result of Sonic's inadequate data security measures and failure to prioritize data security. At the time of the breach, nearly a quarter of Sonic's restaurants used POS systems that were nearly thirty years old. Sonic implemented and utilized operating systems and programs that no longer received security updates, rendering them unable to effectively prevent data breaches.[3] Sonic's deficient security event monitoring failed to successfully identify when its systems were breached and when payment information was being stolen and exfiltrated from its systems.[4] Finally, Sonic deliberately chose not to implement EMV-capable POS systems, a payment card security feature required by the payment card industry and security experts that would have prevented the reuse of stolen payment card information. Following the Sonic Data Breach, Trustwave, a PCI forensic investigator ("PFI") found Sonic violated numerous requirements under the Payment Card Industry Data Security Standards ("PCI DSS"), the *minimum* measures necessary to prevent a breach and limit its scope. Trustwave also determined that payment card information was stolen from 325 Sonic restaurants in 32 states.[5]

---

[2] Settlement Agreement and Release, *In re: Sonic Corp. Customer Data Breach Litig.*, 17-md-02807-JSG, ECF 132 at 1.10 (N.D. Ohio, Oct. 10, 2018).

[3] Plaintiffs' Amended Consolidated Class Action Compl., *In re: Sonic Corp. Customer Data Breach Litig.*, 17-md-02807-JSG, ECF 114 ¶ 44 (N.D. Ohio, July 27, 2018) ("Consumer Compl.").

[4] *Id.* at ¶ 5.

[5] Sonic Defendants' Memorandum Answering the Court's Questions Regarding the Proposed Settlement Agreement and Notice Plan, *In re: Sonic Corp. Customer Data Breach Litig.*, 17-md-02807-JSG, ECF 139 at 3 (N.D. Ohio, July 27, 2018).

8. Although Sonic prioritized new technology in its restaurants, it failed to similarly prioritize new and up-to-date data security measures. Sonic's data security deficiencies and unreasonable data security measures contributed to the breach by both allowing hackers to access Sonic's POS systems and by failing to timely identify the breach and limit its scope.

9. Had Sonic implemented reasonable data security processes and procedures, including those measures known and recommended by the payment card industry, the FTC, and data security experts, Sonic could have reasonably prevented the breach of its systems and the resulting damage.

10. In addition to failing to detect or prevent the data breach and failing to implement data security measures to limit the effect of a breach on cardholders and the financial institutions who issued the payment cards, Sonic exacerbated Plaintiff and the Class's injuries by failing to notify customers of the infiltration when it supposedly learned of the breach in September 2017. In fact, Sonic waited five months to disclose the Sonic locations compromised by the breach.[6]

11. Sonic's data breach forced Plaintiff and other financial institutions to: (a) cancel or reissue credit and debit cards affected by Sonic data breach; (b) close deposit, transaction, checking, or other accounts affected by Sonic's data breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) open or reopen deposit, transaction, checking, or other accounts affected by Sonic's data breach; (d) refund or credit cardholders to cover the cost of unauthorized transactions

[6] Consumer Compl., *supra* note 3, at ¶ 49.

relating to Sonic's data breach; (e) respond to a higher volume of cardholder complaints, confusion, and concern; and/or (f) increase fraud monitoring efforts.

12. In addition, Sonic's data breach caused Plaintiff and the Class to lose revenue as a result of decreased card usage after the breach was disclosed to the public.

13. As alleged herein, the injuries to Plaintiff and the Class were directly and proximately caused by Sonic's failure to implement and maintain adequate and reasonable data security measures necessary for protecting customer information, including credit and debit card data. Sonic failed to take steps to employ adequate security measures despite well-publicized data breaches at large national retail and restaurant chains in recent months, including Target, Home Depot, P.F. Chang's, Eddie Bauer, Wendy's, Dairy Queen, Noodles & Co., Arby's, Chipotle and Kmart.

14. This class action is brought on behalf of financial institutions throughout the United States to recover the costs that they have been forced to bear as a direct result of the data breach of Sonic's systems and to obtain other equitable relief. Plaintiff asserts claims for negligence, negligence per se, and for declaratory and injunctive relief.

## JURISDICTION AND VENUE

15. This Court has original jurisdiction of this Action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332 (d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000 and at least some members of the proposed Class have a different citizenship than Sonic.

16. This Court has personal jurisdiction over Sonic because Sonic maintains its principal place of business in Oklahoma, regularly conducts business in Oklahoma, and has sufficient minimum contacts in Oklahoma. Sonic intentionally availed itself of this

jurisdiction by accepting and processing payments for its services and goods within Oklahoma.

17. Venue is proper under 18 U.S.C. § 1391(a) because Sonic's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

**PARTIES**

18. **Plaintiff** American Airlines Federal Credit Union is a Credit Union headquartered in Fort Worth, TX. AAFCU issues payment cards to its members, who in turn use those payment cards for purchases. AAFCU suffered injury as a result of the Sonic Data Breach in the form of expenses for reissuing impacted cards, covering fraudulent transactions, increased fraud monitoring, and time spent responding to the breach, among other things. Specifically, AAFCU reissued payment cards, reimbursed fraudulent charges, or both as a result of the Data Breach for members residing in California, Florida, Georgia, Illinois, Louisiana, Massachusetts, Minnesota, Nevada, New Hampshire, New Mexico, New York, North Carolina, Ohio, South Dakota, Tennessee, and Washington, among others.

19. **Defendant** Sonic Corp. is a Delaware corporation with its principal place of business or "World Headquarters" at 300 Johnny Beach Dr., Oklahoma City, OK, 73104.

20. **Defendant** Sonic Industries Services, Inc. is a subsidiary of Sonic Corp. and is an Oklahoma corporation with its headquarters and principal place of business in Oklahoma City, Oklahoma.

21. **Defendant** Sonic Capital LLC is a subsidiary of Sonic Corp. and is a Delaware limited liability company with its principal place of business in Oklahoma City, Oklahoma.

22. **Defendant** Sonic Industries LLC is a subsidiary of Sonic Corp. and is a Delaware limited liability company with its principal place of business in Oklahoma City, Oklahoma.

23. **Defendant** Sonic Franchising LLC, is a subsidiary of Sonic Corp. and is a Delaware limited liability company with its principal place of business in Oklahoma City, Oklahoma.

24. **Defendant** Sonic Restaurants, Inc. is a subsidiary of Sonic Corp. and is an Oklahoma corporation with its headquarters and principal place of business in Oklahoma City, Oklahoma.

## ALLEGATIONS

25. Sonic is America's most successful fast food drive-in restaurant. Sonic operates corporate-owned Sonic Drive In restaurants throughout the United States and manages and oversees franchise-owned restaurants, including franchise data security measures. Currently, over 3,600 Sonic restaurants operate in 45 U.S. states, including 345 company-owned restaurants and over 3,000 franchise-owned restaurants.

26. By sales alone, Sonic is the twelfth largest restaurant chain in the United States and the fourth largest quick service burger restaurant chain. Since 2013, Sonic has averaged over half a billion dollars in total revenue annually from both its franchise and corporate restaurants.

27. Although Sonic restaurants are primarily franchise-owned, Sonic Corporate maintains strict control over the technology implemented at both corporate-owned and

franchise restaurants. For example, in 2016, Sonic created a Brand Technology Fund ("BTF") which purportedly sought to administer "cybersecurity and other technology programs for Sonic systems" at both franchise and corporate-owned restaurants.[7] BTF funding is obtained through technology fees paid directly by Sonic restaurants, whether corporate-owned or franchised.[8]

28. Further illustrating Sonic Corporate's control over franchise technology and data security, in 2013, Sonic implemented a full technology revitalization of its in-store and mobile technologies, including new POS systems "designed to boost profitability through improved food cost and labor management" and a Point of Personalized Service platform involving new digital menu boards integrated with mobile and other digital efforts.[9] Sonic Corporate led the effort to institute the technologies included in the revitalization plan at all franchise and corporate-owned restaurants. At the time of the breach, however, nearly a quarter of Sonic's restaurants had not completed the revitalization efforts.[10]

29. Despite implementing a technology "revitalization" plan and establishing the BTF to fund technology advancements, Sonic did not prioritize improving data security measures. In fact, Sonic acknowledged in 2017 that its new POS systems were replacing

---

[7] Annual Report, Sonic at 31 (2016), http://www.annualreports.com/HostedData/AnnualReportArchive/s/NASDAQ_SONC_2016.pdf.

[8] *Id.*

[9] Kara Murphy, *Sonic Rolls Out New POS and POPS Systems*, Retail Insights (Jan. 16, 2014), https://www.retailitinsights.com/doc/sonic-rolls-out-new-pos-and-pops-systems-0001.

[10] Zorrik Voldman, *Sonic Drive-In Is Victim To Security Breach*, 911 Software (Oct. 20, 2017), https://www.911software.com/sonic-drive-in-is-victim-to-security-breach/.

systems that were ***more than 30 years old***.[11] As Matt Schein, Sonic's Vice President of Operations said, "We kind of went from a rotary phone to a smartphone overnight."

30. Sonic's late attempt to replace its "rotary era" technology and data security measures proved insufficient. In 2017, Sonic suffered a data breach resulting in the preventable theft of payment card data from millions of credit and debit cards used at Sonic restaurants. Hackers successfully maneuvered past Sonic's data security measures, and implemented malware on its in-store POS systems, some which may have been from the "rotary-era" systems and some which may have been Sonic's newer models. Overall, Sonic allowed hackers to access millions of customers' payment card information through malware infecting systems at 325 locations in 32 states.

***Sonic Was On-Notice of the Vulnerabilities of POS Systems***

31. Sonic knew or should have known its POS systems would be a target for hackers, and that a breach of its corporate network security would permit hackers to install malware at locations throughout the U.S., putting millions of customers at risk of having their payment card data stolen. Indeed, the theft of payment card information via POS systems has long been "one of the biggest sources of stolen payment cards."[12]

32. A POS system provides the hardware, software, and networks responsible for facilitating payments made by credit and debit cards. At a POS terminal, "data contained in [a payment] card's magnetic stripe is read and then passed through a variety

[11] Ron Ruggless, *Sonic team helps operators reap benefits of new POS system*, Nation's Restaurant News (Apr. 14, 2017).

[12] Symantec, *A Special Report On Attacks On Point-of-Sale Systems* 3 (Nov. 20, 2014), https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf.

of systems and networks before reaching the retailer's payment processor."[13] The payment processor completes the transaction by passing payment information to the appropriate Card Brand (Visa, MasterCard, etc.) networks and then to the financial institution that issued the card for approval of the transaction.[14] Once approved, the retailer is paid by an acquiring or merchant bank, and the issuing bank later reimburses the acquiring bank for the transaction.

33. To send payment card information to the payment processor, businesses use a Cardholder Data Environment, usually referred to as a CDE or a CHDE.[15] The CDE is a part of the POS system and represents the network that transfers card information from the POS terminal to the payment processor who assists with authorizing the transactions. Elements of the CDE include all network components like firewalls, switches, routers, access points, and network appliances, POS systems, servers, and often virtual components like virtual machines, switches, routers, desktops and hypervisors.[16]

[13] *Id.* at 6.

[14] Slava Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions 8 (Wiley 2011).

[15] *Id.* at 39.

[16] *Cardholder Data Environment (CDE)*, TechTarget.com (last visited, Jan. 2, 2019) (noting "[m]ost data breaches in teh retail sector involve a compromise of the cardholder data network."), https://searchsecurity.techtarget.com/definition/cardholder-data-environment-CDE

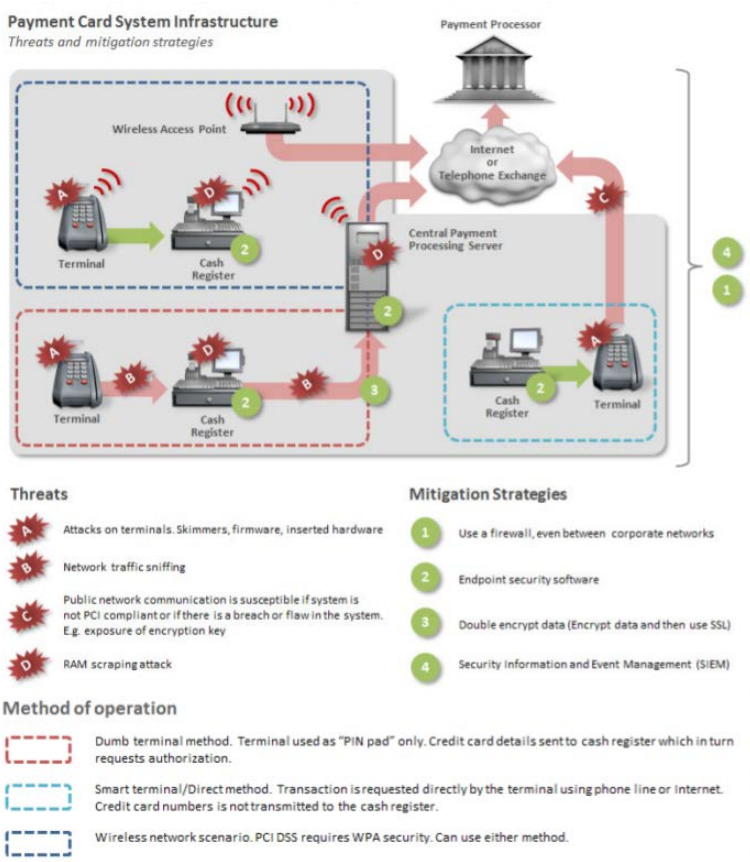


***Figure 1.*** **An example of a CDE and its vulnerabilities.**

34. When hackers gain access to POS systems, they have direct access to payment card information. Before transmitting consumer purchasing information over the network through the deployment architecture, the POS system typically, very briefly, stores data from the card's magnetic stripe in unencrypted plain text within the POS system's memory before transfer or encryption.[17] Stored payment information includes "Track 1" and "Track 2" data—originally stored on the magnetic stripe of the payment card—which includes the full information about the cardholder, including first and last name, the expiration date of the card, and the CVV (three number security code on the card).[18] This

[17] Symantec, *supra* note 12, at 6.

[18] Gomzin, *supra* note 14, at 98-101.

information is unencrypted on the card and, if left unencrypted on the POS device, is easily accessible by hackers using common malware.[19] Hackers with access to Track 1 and Track 2 payment card data can physically replicate the card for in person use or can use the data to make fraudulent purchases online.

35. To gain access to POS systems, hackers generally use four general steps: infiltration, propagation, exfiltration, and aggregation.[20] In the infiltration phase, an "attacker gains access to the targeted environment[,]"[21] which normally includes hacking into a business's corporate network and finding an entry point into the CDE. To access the corporate network, hackers use phishing attacks which "trick[] or bait[] employees into giving access to the company's network."[22] Phishing emails typically seek to fool employees into opening malicious attachments or unknowingly providing their login information to the nefarious actors. Using the employee's credentials, the hackers finds vulnerabilities in the corporate network or attempts to obtain administrative privileges to obtain access to the CDE. The CDE is directly connected to the physical POS machines at in-store locations, and therefore, once a hacker breaches the CDE, the hacker may access the POS systems and terminals at in-store locations.[23] In the second phase, the attacker then

[19] Symantec, *supra* note 12, at 5.

[20] *Point of Sale Systems and Security: Executive Summary*, SANS Institute 4 (Oct. 2014), https://www.sans.org/reading-room/whitepapers/analyst/point-sale-systems-security-executive-summary-35622

[21] *Id.*

[22] Trend Micro, *Data Breaches 101: How They Happen, What Gets Stolen, and Where it Goes*, Trendmicro.com (Aug. 10, 2018), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

[23] Symantec, *supra* note 12, at 6.

infects or propagates the POS systems with malware.[24] The malware "collects the desired information . . . and then exfiltrates the data to another system[,]" called the "aggregation point."[25] From the aggregation point, payment data is transferred to a system outside the target environment, where it can be retrieved.[26]

36. According to one report, "[t]he vast majority of successful breaches leverage legitimate credentials to gain access to the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to capture payment card data."[27] Hackers, on average, successfully compromise unsecured POS systems in a matter of minutes or hours and exfiltrated data within days of placing malware on the POS devices.[28]

37. Sonic knew or should have known hackers would target its POS systems to obtain customer payment card information. Since 2013, malware installed on POS systems has been responsible for nearly every major data breach of a retail outlet or chain restaurant. In 2015 alone, data breaches into POS systems accounted for 64% of *all* breaches where hackers successfully stole data.[29] In 2014, retail entities replaced credit, banking and financial institutions as the leader in greatest number of data breaches experienced per year

[24] SANS, *supra* note 20, at 4.

[25] *Id.*

[26] *Id.*

[27] *See, e.g., 2016 Data Breach Investigations Report*, Verizon at 1 (Apr. 2016), http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Retail-Data-Security_en_xg.pdf

[28] *Id.* at 4.

[29] *Id.* at 3.

and by far, the most common means of data theft is through hacking, phishing, or skimming schemes targeting POS systems.[30]

38. These breaches have resulted in hundreds of millions of compromised payment cards,[31] and the number of breaches has continued to increase.[32] Since the 2014 Target Data Breach, the media has reported data breaches at numerous businesses and other chain restaurants, including: Neiman Marcus, Michaels, Sally Beauty Supply, P.F. Chang's China Bistro, Eddie Bauer, Goodwill, SuperValu Grocery, UPS, Home Depot, Jimmy John's, Dairy Queen Restaurants, Staples, Kmart, Noodles & Co., GameStop, Wendy's, Chipotle and Arby's, among others. These breaches have been well publicized and most or all involved RAM scraping POS malware similar to that employed in the Sonic Data Breach. Given the numerous, well-publicized retail outlet and fast-food data breaches, Sonic was on notice that its POS systems would be targeted and a breach could led to the theft of millions of customers' payment card information.

39. The Wendy's data breach in particular should have been a massive warning sign for Sonic that it may be vulnerable to a breach. In 2016, hackers compromised Wendy's Restaurants' POS systems using malware capable of stealing consumer purchasing information. Hackers gained entry into Wendy's POS machines at franchise-owned restaurants through similar methods used in the Target breach: compromised credentials provided to a third-party service provider with remote access to Wendy's

---

[30] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScourt*, Identity Theft Resource Center (Jan. 19, 2017), http://www.idtheftcenter.org/2016data-breaches.html.

[31] Symantec, *supra* note 12, at 3.

[32] *See* Identity Theft Resource Center, *supra* note 30.

franchise networks and restaurants.[33] Once hackers had access to Wendy's networks, they deployed malware onto POS terminals at franchisee-locations which ultimately collected consumer payment data.[34] At least one security expert believed EMV chip readers at franchisee locations would have prevented some theft of payment data.[35] Although Wendy's discovered its franchise-owned restaurants were breached, it failed to identify the full scope of the breach and thus, failed to fully remediate the data breach. For more than six months, hackers stole payment card information from certain Wendy's franchise restaurants before Wendy's fully identified and remediated the breach.[36] The divide between Wendy's Corporate and Wendy's franchisees created specific vulnerabilities in the data security of Wendy's as a whole. Because Sonic Corporate manages primarily franchise-owned systems and directs those restaurants data security measures, the severity and scope of Wendy's data breach should have put Sonic on notice of the vulnerability of its own operations.

40. Additionally, data security experts have specifically and publicly warned businesses, like Sonic, about the threats of data breaches in the quick-service food industry. One expert warned that "overall fraud rates [in the food service industry] have risen by 13 percent since [2016]." [37] "[T]he threat is serious. Beyond POS systems, fraudsters often go

---

[33] *Wendy's Update on Payment Card Security Incident*, Wendys.com (last visited, Apr. 26, 2017), http://ir.wendys.com/phoenix.zhtml?c=67548&p=irol-newsArticle&ID=2182670

[34] *Id.*

[35] Brian Krebs, *1,025 Wendy's Locations Hit in Card Breach*, KrebsOnSecurity (July, 16, 2016), https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/#more-35408.

[36] *Id.*

[37] Michael Reiblat, *Is your restaurant data-breach proof?*, Fast Casual (Aug. 3, 2018), https://www.fastcasual.com/blogs/is-your-restaurant-data-breach-proof.

directly to the source by attacking the restaurant's network or computer system, which stores files containing sensitive financial details. POS network attacks can affect multiple chain locations simultaneously and expose immense quantities of data in one fell swoop, allowing attackers to remotely steal data from each credit card as it is swiped at the cash register."[38] However, these data breaches are preventable: "To help prevent fraud attacks, restaurants need to ensure they comply with the standards governing the handling of payment card information, . . . manage the risks associated with third party vendors and put an effective incident response plan into place."[39]

41. In 2015, the National Restaurant Association warned that restaurants that hackers "prey on businesses that are ill-prepared for an attack" and advised that "[j]ust as you have made food safety an integral part of your quality assurance program, you need to also make cybersecurity a part of your operation."[40] The Association admonished that "you're never finished" improving data security measures.[41] "[C]ybersecurity is not about checking boxes . . . Rather, cybersecurity is a continual process that you need to build into your daily operations. Threats will change, but if your cybersecurity program is designed properly, you'll be able to respond accordingly and adopt new policies to reduce the risk of cyberattacks. Remember, there are no shortcuts."[42]

---

[38] *Id.*

[39] *Id.*

[40] *Cybersecurity 101: A Toolkit for Restaurant Operators*, Nat'l Restaurant Assoc. 1 (2016), https://www.restaurant.org/Downloads/PDFs/advocacy/cybersecurity101.pdf.

[41] *Id.* at 4.

[42] *Id.*

42. These warnings, among others, put Sonic on notice that it may be susceptible to a data breach and of the importance of prioritizing data security to prevent a breach. Despite Sonic's knowledge of the likelihood that its customers' payment card information would be stolen without reasonable security measures, and that its CDE and POS systems were a target of hackers, Sonic implemented woefully inadequate data security measures that allowed hackers to easily penetrate its systems and steal payment card information.

***Hackers Accessed Sonic's Point-of-Sale Systems Due to Its Unreasonable Security Measures***

43. Sonic is, and at all relevant times was, aware that the payment card data it receives via credit and debit card transactions is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. Sonic knew of the necessity of safeguarding payment card data and of the foreseeable consequences that would occur if its data security systems were breached, including the significant costs that would be imposed on issuers, such as the Plaintiff and members of the Class. Numerous widely-reported retail and fast-food chain data breaches put Sonic on notice of the means by which hackers infiltrate POS systems and obtain payment card data.

44. Sonic is, and at all relevant times was, fully aware of the significant volume of daily credit and debit card transactions at Sonic's franchise restaurants, amounting to tens of thousands of daily credit card transactions, and thus, the significant number of individuals and businesses who would be harmed by a breach of Sonic's POS systems.

45. Although Sonic understood the need for implementing reasonable data security measures, it failed to do so. In 2017, hackers breached Sonic's data security

systems and infected POS systems at 325 restaurants in 32 states, stealing information on an estimated five million payment cards.[43]

46. Sonic's Data Breach became public after Brian Krebs, a data security expert and journalist, investigated claims by "multiple financial institutions" regarding a pattern of recent fraudulent transactions traceable to payment cards used at Sonic.[44] Krebs identified over five million credit cards placed on the website "Joker's Stash," a dark website that facilitates the sale of stolen credit cards. According to Krebs, multiple banks purchased batches of the stolen credit cards and determined these cards had recently been used at Sonic locations.

47. Krebs contacted Sonic to inform them of the potential data breach. Sonic confirmed to Krebs that it was investigating a data breach of its POS systems. Sonic wrote:

> Our credit card processor informed us last week of unusual activity regarding credit cards used at SONIC . . . The security of our guests' information is very important to SONIC. We are working to understand the nature and scope of this issue, as we know how important this is to our guests. We immediately engaged third-party forensic experts and law enforcement when we heard from our processor. While law enforcement limits the information we can share, we will communicate additional information as we are able.[45]

48. Krebs reported that hackers likely accessed Sonic's POS systems and used malware to gather payment card information, which the hackers later sold to cybercriminals on Joker's Stash for the purpose of using the payment card data to make fraudulent transactions.

---

[43] Brian Krebs, *Breach at Sonic Drive-In May have Impacted Millions of Credit, Debit Cards*, KrebsOnSecurity (Sep. 26, 2017), https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/

[44] *Id.*

[45] *Id.*

49. The data breach resulted from Sonic's unreasonable and negligent data security standards. Sonic admitted publicly that many of its POS systems were decades old, a massive failure considering the fast growing and advanced hacking techniques that have developed over the past decade alone.[46] Indeed, Sonic recognized as early as 2013 that it needed to replace and revamp its POS systems, a project that it had not completed by 2017, four years after its inception and long after its original target dates.[47] By the time of the breach, Sonic had converted approximately 77% of its POS systems, but the remainder used outdated, older systems and terminals.[48]

50. One anonymous individual claiming to be a former Sonic employee recounted that Sonic's "[a]ntiquated Software caused [the] Breach." [49] The individual wrote that Sonic's "Executives [were] too focused on delivering unnecessary . . . 'new apps' instead of fixing a problem they were all aware of, [and the] end result [is] millions of customers impacted, [s]tock prices go down, more layoffs to come[.]"[50] The individual's view aligns with Sonic's repeated emphasis on new technologies but complete lack of security-driven projects.

51. Sonic's Vice President of Public Relations, Christi Woodworth, also stated that Sonic "ha[d] not adopted EMV for a variety of reasons specific to our business."[51]

---

[46] Jeremy Kirk, *Fast-Food Chain sonic Investigates Potential Card Breach*, Bank Info Security (Sep. 27, 2017), https://www.bankinfosecurity.com/sonic-drive-in-investigating-possible-card-breach-a-10337

[47] *See* Murphy, *supra* note 9.

[48] *See* Voldman, *supra* note 10.

[49] *Sonic Corp. Layoffs*, The Layoff (last visited Dec. 4, 2018), https://www.thelayoff.com/t/PLisqcZ

[50] *Id.*

[51] Kirk, *supra* note 46.

EMV, which stands for Europay Mastercard and Visa, is a type of payment card where payment information is generated by a computer chip embedded within the card. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data where a unique transaction code is created for each transaction and cannot be used again. When payment card information from an EMV transaction is stolen, the unique payment information typically cannot be used by the hackers, making it much more difficult for criminals to profit from what is stolen.

52. Apart from failing to prevent hackers from infiltrating its CDE, Sonic also failed to identify the fact hackers had installed malware onto its POS systems and were exfiltrating payment card information. Real-time monitoring systems are designed to provide alerts to business when their systems are breached and information is being stolen. Sonic's outdated monitoring systems failed to adequately alert Sonic of the scope of the breach, and even when alerts were generated, Sonic either ignored them or failed to fully review them.[52] Had Sonic utilized sufficient monitoring tools and sufficiently reviewed alerts generated by its monitoring tools, it would have identified the breach much sooner, resulting in far fewer compromised payment cards. Adequate real-time monitoring may have prevented the exfiltration of PCI entirely.

53. The Sonic breach may have continued even longer if payment card industry investigators had not noticed unusual activity on payment cards used at Sonic restaurants or if those investigators had not linked stolen credit card information on the internet to Sonic locations. In other words, Sonic was entirely oblivious to the breach until outside third-parties informed it of the breach.

[52] Consumer Compl., *supra* note 3, at ¶¶ 5, 63.

54. Although Sonic has not stated the length of the exposure window, its settlement with the consumer class suggests Sonic was breached from April through almost all of October, more than half a year long.[53] The exposure window lasted forty days after Sonic purportedly learned of the breach on September 18, 2017, indicating it failed to timely remediate its systems.

55. Sonic's public response to the breach was likewise woefully inadequate. Sonic waited until October 4, 2017, more than two weeks after it learned of the breach, to provide any public notice. Although Sonic knew cards compromised at its restaurants were being sold on Joker's Stash, it downplayed the extent of the breach, stating "credit and debit card numbers *may* have been acquired without authorization."[54] At that time, Sonic provided no information about the scope or extent of the breach and did not indicate which restaurant locations were impacted.[55] In fact, Sonic waited five months to announce which Sonic locations had been impacted by the data breach.[56]

56. Sonic eventually issued a revised public announcement which listed the addresses of the 325 locations it identified as having been compromised. [57] Sonic has still provided no public information about the timeline of the data breach.

57. After the breach, the Card Brands required Sonic to use a private forensic investigator, Trustwave, to investigate the cause of the Data Breach. Trustwave identified

---

[53] Settlement Agreement and Release, *supra* note 2, at 1.10.

[54] Consumer Compl., *supra* note 3, at ¶ 47.

[55] *Id.*

[56] *Id.*

[57] *Notice of Data Breach*, SonicDriveIn.com (last visited, Dec. 10, 2018), https://www.sonicdrivein.com/-/notice-of-data-breach

a host of basic data security measures that Sonic lacked before and during the breach, including some that directly contributed to the breach, and many that qualified as violations of the PCI DSS, the Payment Card Industry's required data security measures.[58] Trustwave found Sonic used out-of-date computer systems and data security practices, including systems that used end-of-life ("EOL") software and hardware and systems that lacked point-to-point encryption ("P2PE").[59] EOL is a term of art in the data security field indicating that a piece of software is no longer receiving updates or patches from the developer making it vulnerable to new data security threats. P2PE is a technique that would limit the ability of hackers, even those who had access to POS systems, to obtain meaningful payment card information from those systems and has been a basic data security measure recommended by data security experts for years.

58. Ultimately, Sonic enacted unreasonable data security measures that permitted hackers to easily enter its corporate network, CDE, and POS Systems. Then, because Sonic failed to implement reasonable security monitoring measures, the breach continued unnoticed until an estimated 5 million payment cards were compromised. The exposure window described in Sonic's data breach settlement with consumers suggests the data breach lasted from April 7, 2017 to October 28, 2017, meaning hackers infiltrated, resided in, and exported data from Sonic's systems for months without notice. The Sonic Data Breach and the resulting payment card theft was preventable had Sonic implemented reasonable, industry-recommended data security standards. However, it failed to do so.

***Sonic's Unreasonable Data Security Measures Failed to Comply with Known Data Security Protocols***

[58] Consumer Compl., *supra* note 3. at ¶ 44, 50-54, 57.

[59] *Id.* at ¶¶ 2, 44, 57, 114.

59. Sonic should have been on high alert to the susceptibility of POS systems to data breaches. Security experts have consistently warned about the susceptibility of POS systems in restaurants.[60] One expert warned businesses that "you can't neglect POS system security" noting that "[a]ny POS terminal with an IP address and a connection to a business's network is as vulnerable to compromise as all the other pieces of equipment in that network."[61] The same expert stated "[i]t's not only okay to be obsessive about testing your POS systems for vulnerabilities and compromises…it's essential."[62]

60. Datacap Systems, Inc. wrote in early 2016, "[y]our POS system is being targeted by hackers. This is a fact of 21st-century business."[63] The same article notes Verizon reported "99 percent of the time, POS environments were hacked in only a few hours . . . [and] in 98 percent of cases, hackers exfiltrated data in just a couple of days." The reason for the number and significance of data breaches was "[s]imply put, too many businesses . . . practicing less-than-stellar POS security."[64]

61. Specific measures and businesses practices can reduce the likelihood hackers can successfully intrude into businesses' POS systems and limit the effect of any malicious software installed on any POS system or device. In fact, the Online Trust Alliance, a non-profit organization whose mission is to enhance online trust, user empowerment, and

---

[60] Leebro POS, *5 Lessons To Learn From A Restaurant POS Security Breach*, Pointofsale.com (last visited, Feb. 28, 2017), https://pointofsale.com/201506256716/Restaurant/Hospitality/5-Lessons-to-Learn-from-a-Restaurant-POS-Security-Breach.html.

[61] *Id.*

[62] *Id.*

[63] *See* Datacap Systems, *supra* note 1.

[64] *Id.*

innovation, in its 2015 annual report, revealed that 90% of data breaches in 2014 were preventable.[65] Similarly, in 2017, the Online Trust Alliance found more than 93% of incidents in 2016 were preventable.[66] The OTA emphasized that "[o]rganizations must make security a priority" and "those that fail will be held accountable."[67]

62. More than three years ago, a Symantec report listed vulnerabilities in POS systems that should be resolved to prevent entry into POS systems and theft of consumer purchasing information.[68] First, Symantec recommended "point to point encryption" implemented through secure card readers which encrypt credit card information in the POS system, preventing "RAM-scraping" malware which extracts card information through the POS memory while it processes the transaction. Second, Symantec highlighted the need to utilize updated software to avoid susceptibility in older operating systems being phased out, like Windows XP or Windows XP Embedded. Third, Symantec emphasized the need to implement POS systems capable of accepting EMV chips in payment cards, preventing the directly transmission of credit card information. These basic data security measures, known long before the Sonic data breach, are still important for preventing data breaches today.

---

[65] Press Release, *OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented*, Online Trust Alliance (Jan. 21, 2015), https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented.

[66] Bradley Barth, Report: Number of Cyber Incidents Doubled in 2017, Yet 93 Percent Could Easily Have Been Prevented, SC Media (Jan. 28, 2018), https://www.scmagazine.com/home/security-news/privacy-compliance/report-number-of-cyber-incidents-doubled-in-2017-yet-93-percent-could-easily-have-been-prevented/

[67] Online Trust Alliance, *supra* note 65.

[68] *See* Symantec, *supra* note 12, at 11-12.

63. Datacap Systems recommends similar preventative measures in what they call the "Tripod of POS Security."[69] The "tripod" includes (1) implementing POS systems supporting EMV chip-based payment cards; (2) end-to-end encryption, which encrypts payment card data as soon as payment cards are swiped; and, (3) tokenization, which replaces credit and debit card numbers with meaningless series of letters and numbers, rendering any information collected by hackers meaningless.

64. Notably, at the time of the breach, Sonic's restaurants were not in compliance with *any* of Symantec's or Datacap Systems' basic data security requirements. Sonic did not use point-to-point encryption in all of its restaurants; some of Sonic's computers were EOL and no longer supported with security patches; Sonic did not use EMV-capable POS systems; and, Sonic did not use tokenization to mask the credit and debit card information.

65. The payment card industry (including card brands MasterCard, VISA, Discover, JCB, and American Express) has also heightened security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; (3) comply with all industry standards.

66. The PCI Security Standards Council, founded by American Express, Discover, JCB, MasterCard, and VISA, promulgates data security standards (again, referred to as "PCI DSS") developed to "encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures." PCI DSS applies "to all entities involved in payment card processing—including merchants, processors,

[69] *See* Datacap Systems, *supra* note 1.

acquirers, issuers, and service providers. PCI DSS comprises "a minimum set of requirements for protecting data."

67. PCI DSS 3.2, the version of the standards in effect at the time of the Sonic Data Breach, sets forth twelve detailed and comprehensive requirements that must be followed to meet six data security goals:

**The PCI Data Security Standard**

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps th mirror security best practices.

| Goals | PCI DSS Requirements |
|---|---|
| Build and Maintain a Secure Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | 3. Protect stored cardholder data<br>4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Protect all systems against malware and regularly update anti-virus software or programs<br>6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need to know<br>8. Identify and authenticate access to system components<br>9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data<br>11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for all personnel |

68. Among other things, the PCI DSS required Sonic to: properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data on a need-to-know basis; establish a process to identify and timely fix

security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and encrypt payment card data at the point of sale.

69. Compliance with PCI DSS is required, but comprises only a portion of the minimum protective action a business must take. Security experts warn that "[w]hile PCI DSS provides a framework for improved payment processing, it is clear that it has been insufficient to ensure the security of modern retail POS systems. To truly improve the security posture of POS devices, organizations must take a more dynamic approach."[70] In fact, "every company that has been spectacularly hacked in the last three years has been PCI compliant."[71] Target, Home Depot, Neiman Marcus, Michael's, Sally Beauty Holdings, Inc., Supervalu, Albertson's and many other businesses subjected to data breaches were recognized as PCI DSS compliant at the time of the compromise.[72]

70. Federal and State governments have likewise sought to introduce security standards and recommendations to temper data breaches and resulting harm to consumers and financial institutions. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor security into all business decision-making.[73] Data security requires encrypting information stored on computer networks; holding on to information only as long as necessary; properly disposing of personal information that is no longer needed; limiting administrative access

---

[70] SANS, *supra* note 20, at 1.

[71] Sean M. Kerner, *Eddie Bauer Reveals It Was the Victim of a POS Breach*, eWeek (Aug. 19, 2016), http://www.eweek.com/security/eddie-bauer-reveals-it-was-the-victim-of-a-pos-breach.html.

[72] SANS, *supra* note 20, at 1.

[73] Federal Trade Comm'n, *Start With Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

to business systems; using industry-tested and accepted security methods; monitoring activity on your network to uncover unapproved activity; verifying that privacy and security features work; testing for common vulnerabilities; and, updating and patching third-party software.[74]

71. The FTC has also taken an active approach in issuing orders against businesses for failing to adequately and reasonably protect customer data. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. The FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data.[75] These orders further clarify the measures businesses must take to meet their data security obligations.

72. Several states have specifically enacted data breach statutes requiring merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code §1798.81.5(b) and Wash. Rev. Code §19.255, or that otherwise impose data security obligations on merchants, such as the Minnesota Plastic Card Security Act, Minn. Stat. §325E.64. States have also adopted unfair and

---

[74] *See id;* Federal Trade Comm'n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[75] *See, e.g., FTC v. Wyndham Worldwide Corp., et al.*, No. 13:-CV-01887-ES-JAD (D. N.J. December 11, 2015); *In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH) ¶ 79708 (MSNET July 28, 2016); *In the Matter of Gmr Transcription Servs., Inc.*, 2015-1 Trade Cas. (CCH) ¶ 17070 (MSNET Aug. 14, 2014); *In the Matter of Genelink, Inc.*, 2015-1 Trade Cas. (CCH) ¶ 17034 (MSNET Jan. 7, 2014).

deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. Oklahoma's Consumer Protection statute, for example, prohibits business from "commit[ing] an unfair or deceptive trade practice." 15 OK Stat. § 15-753(20). Most states, including Oklahoma, have also enacted statutes requiring merchants to provide notice to consumers of security systems breaches. *See* 24 OK Stat. § 24-163. These statutes, implicitly or explicitly, mandate the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

73. In this case, Sonic was at all times fully aware of its data protection obligations for all Sonic franchise and restaurant locations because of, among other reasons, its participation in payment card processing networks. Sonic also knew of the significant repercussions of a data breach because of the numerous daily transactions of tens of thousands of sets of payment card data. Sonic further knew that because they accepted payment cards at Sonic restaurant locations which processed sensitive financial information, customers and financial institutions, including Plaintiff and the Class, were entitled to and relied upon Sonic to keep sensitive information secure from hackers.

74. Despite understanding the consequences of a data breach and the measures it could take to avoid a data breach, Sonic failed to comply with PCI DSS requirements; failed to take additional protective measures beyond the PCI DSS; failed to implement EMV-capable POS systems by the October 1, 2015 deadline; operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take necessary protective measures on its corporate network.

75. The culmination of Sonic's failed security measures was the breach of its POS systems at its corporate-owned restaurants, franchise restaurants or both, allowing

hackers to compromise almost 300 restaurants, resulting in the theft of information on over 5 million payment cards.

76. Sonic failed to reasonably protect cardholder information, putting consumer financial accounts in jeopardy and forcing financial institutions, like Plaintiff and the Class, to take remedial action for Sonic's inadequate preventative security measures.

77. Sonic had every opportunity to take preventive measures to avoid a breach of its POS systems. First, Sonic had more than adequate notice about the potential for hackers to infiltrate POS systems and rob customers of their credit and debit card information. Second, Sonic appreciated the consequences of such a breach, having witnessed Wendy's, Arby's and other major competitors experience data breaches in 2016 and 2017 and others like Target and Home-Depot experience breaches between 2013 and 2014. Third, Sonic had access to information from data security experts, the FTC, and the payment card industry identifying steps necessary to protect POS systems. Fourth, Sonic had available established guidelines from PCI DSS that offered at least, minimal levels of protection. Fifth, Sonic had recently replaced its POS systems and designed a Brand Technology Fund to fund technology enhancements. Despite the resources indicating the degree of risk of POS data breach and the potential steps to stymie a data breach, Sonic failed to take reasonable and sufficient action to avoid a breach of its POS systems, including failing to meet even minimal data security requirements. While Sonic saved money by deliberately truncating its data security investments, it knowingly put itself at risk of a breach and Plaintiff at risk of incurring expenses necessary to remediate and limit the damages caused by a breach.

78. Had Sonic remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Sonic may

have prevented data breach into its POS systems and ultimately, the theft of millions of customers' purchasing information.

79. Because Sonic failed to take reasonable protective measures to prevent a data breach, Plaintiff and the Class will be required to bear the costs of preventing and repaying fraudulent transactions made with credit and debit card information obtained through Sonic's POS systems.

80. As a direct and proximate result of Sonic's Data Breach, Plaintiff and the Class have suffered damages and injuries, including expenses related to the following: (a) cancelling or reissuing credit and debit cards affected by the Sonic Data Breach; (b) closing any deposit, transaction, checking, or other accounts affected by Sonic's data breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) opening or reopening any deposit, transaction, checking, or other accounts affected by Sonic's data breach; (d) refunding or crediting cardholders to cover the cost of any unauthorized transactions relating to Sonic's data breach; (e) responding to a higher volume of cardholder complaints, confusion, and concern; (f) increasing fraud monitoring efforts; and (g) investigating the impact of the breach on the financial institution and its members.

81. In this case, Sonic's data breach compromised an estimated 5 million payment cards. The Credit Union National Association ("CUNA") estimates the average cost to reissue payment cards is $8.02[76], meaning financial institutions may have spent as

[76] *Visa tiers reimbursement costs for reissuing breached cards*, Credit Union Nat'l Assoc. (May 21, 2015), https://news.cuna.org/articles/106029-visa-tiers-reimbursement-costs-for-reissuing-breached-cards.

much as $40.1 million in card reissuance costs alone as a result of the data breach. The cost may be even greater for EMV cards, which are more expensive to replace.

82. Additionally, because the payment card information stolen from Sonic and offered on Joker's Stash was new – indicating it pre-dated knowledge of the breach – the risk of fraudulent charges is increased because financial institutions, like Plaintiff and the Class, did not have the opportunity to preemptively cancel and reissue cards upon receipt of an alert from the Card Brand (Visa, Mastercard, Discovery, and American Express) of potentially fraudulent activity or of a potentially compromised card. Without advance notice, purchasers of the stolen payment card information had a prolonged period to use or replicate the payment cards and make fraudulent purchases.

83. The Sonic Data Breach, therefore, likely cost Plaintiff and the Class tens-of-millions of dollars in actual expenses for remediating and mitigating the damages it caused.

## CLASS ALLEGATIONS

84. Plaintiff brings this action on behalf of itself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seeks certification of the following Nationwide Class:

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases at Sonic's restaurants during the Sonic Data Breach.

85. Excluded from the class is Defendant and its subsidiaries and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

86. Plaintiff reserves the right to modify, expand or amend the above class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate following discovery.

87. **Numerosity**. Consistent with Rule 23(a)(1), the members of the classes are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are thousands of members of the Class and the sheer number of alerts notifying financial institutions of compromised card payment information indicates the Class is numerous; however, the precise number of class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

88. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Sonic knew or should have known of the susceptibility of its POS systems to a data breach;

b. Whether Sonic's security measures were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and common recommendations made by data security experts;

c. Whether Sonic owed Plaintiff and the Class a duty to implement reasonable security measures;

d. Whether Sonic's failure to adequately comply with PCI DSS standards and/or to institute protective measures beyond PCI DSS standards amounted to a breach of its duty to institute reasonable security measures;

e. Whether Sonic's failure to implement reasonable data security measures allowed the breach of its POS data systems to occur;

f. Whether reasonable security measures known and recommended by the data community could have reasonably prevented the breach of Sonic's POS systems;

g. Whether Sonic failed to adequately notify Plaintiff and the Class that its systems were hacked and payment card data was stolen;

h. Whether Sonic acted unfairly and deceptively by utilizing unreasonable data security measures and knowingly placing the risk of a data breach on Plaintiff and the Class;

i. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Sonic's failure to reasonably protect its POS data systems and corporate network;

j. Whether Plaintiff and the Class are entitled to relief;

89. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff is a credit union which issued payment cards compromised by the infiltration and theft of card payment information from Sonic's POS system. Plaintiff's injuries are similar to other class members and Plaintiff seeks relief consistent with the relief of the Class.

90. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Sonic to obtain relief for itself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

91. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this

controversy, Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit financial institutions to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

92. Injunctive and Declaratory Relief. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

## CLAIMS

### COUNT I
### Negligence

93. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

94. Sonic owed an independent duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting payment card information. This duty arises from multiple sources.

95. At common law, Sonic owed an independent duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that Sonic's data systems and the payment card data those systems processed would be targeted by hackers and that, should a breach occur, Plaintiff and the Class would be harmed. Sonic

knew or should have known that if hackers had breached its data systems, they would extract payment card data and inflict injury upon Plaintiff and the Class. Furthermore, Sonic knew or should have known that if hackers accessed payment card data, Plaintiff and the Class would be responsible for remediating and mitigating the consequences of a breach by cancelling and reissuing payment cards to their members and reimbursing their members for fraud losses, thereby incurring costs and damages as a direct result of Sonic's breach. Therefore, the foreseeable consequence of Sonic's unsecured, unreasonable data security measures was a data breach that harmed Plaintiff and the Class.

96. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Sonic to take reasonable measures to protect cardholder data. Section 5 prohibits unfair practices in or affecting commerce, which required and obligated Sonic to take reasonable measures to protect payment card data Sonic may possess, hold, or otherwise use. The FTC publications and data security breach orders described herein further form the basis of Sonic's duty to adequately protect sensitive card payment information. By implementing unreasonable data security measures, Sonic acted in violation of § 5 of the FTCA. Moreover, state consumer protection statutes and deceptive and unfair trade practices statutes, incorporate and prohibit the unfair conduct prohibited under § 5 of the FTCA.

97. Sonic is obligated to perform its business operations in accordance with industry standards, including the PCI DSS, to which Sonic is bound. Industry standards are another source of duty and obligations requiring Sonic to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

98. Sonic breached its duty to Plaintiff and the Class. Specifically, Sonic implemented unreasonable data security measures, including failing to utilize adequate systems, procedures, and personnel necessary to prevent the disclosure and theft of the cardholder data of Plaintiff and the Class's members. Sonic's unreasonable actions include violating PCI DSS by using technologies that were no longer supported by security patches, failing to utilize EMV-capable POS systems, implementing ineffective security monitoring technologies and procedures, failing to implement point-to-point encryption, and other unreasonable data security measures that foreseeably caused the data breach and which Sonic knew or should have known were unreasonable.

99. Sonic was fully capable of preventing the data breach. Sonic knew of data security measures required or recommended by the PCI DSS, FTC, and other data security experts which, if implemented, would have prevented the data breach from occurring at all, or, even if its POS systems were compromised, would have limited the scope and length of the breach. Sonic established a Brand Technology Fund specifically to fund technology initiatives, which should have, but did not, include data security projects. Sonic failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

100. As a direct and proximate cause of Sonic's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including, but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

101. Because no statutes of other states are implicated, Oklahoma common law applies to Plaintiff and the Class's negligence claim.

**COUNT II**
**Negligence *Per Se***

102. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

103. Sonic's unreasonable data security measures and failure to timely notify consumers of the Data Breach violate Section 5 of the Federal Trade Commission Act ("FTCA"), the Oklahoma Breach Notification Act ("OBNA"), and the Oklahoma Consumer Protection Act ("OCPA"). Although neither the FTCA nor the OBNA create a private right of action, both require businesses to institute reasonable data security measures and breach notification requirements, which Sonic failed to do. Similarly, the OCPA prohibits businesses from acting unfair or deceptively.

104. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, restaurants and other businesses like Sonic of failing to use reasonable measures to protect cardholder data. The FTC publications and orders described above also form the basis of Sonic's duty.[77]

105. Sonic violated Section 5 of the FTCA by failing to use reasonable measures to protect cardholder data and by not complying with applicable industry standards, including PCI DSS. Sonic's conduct was particularly unreasonable given the nature and amount of payment card data it obtained and the foreseeable consequences of a data breach at a national restaurant, including specifically the immense damages that would result to consumers and financial institutions like Plaintiff and the Class.

[77] *See supra*, note 75 (listing orders).

106. Sonic's violation of Section 5 of the FTCA constitutes negligence per se.

107. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect because they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, Plaintiff and many class members are credit unions, which are organized as cooperatives whose members are consumers.

108. Additionally, the harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

109. The OBNA states "Federal and State Laws require that if you maintain . . . a consumer's name and other personal identification numbers" including "credit card or financial information," such information is required to be "encrypted or redacted so that in the event of a breach, such information cannot be obtained and used by a third party." Additionally, the Act states:

> An individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this state whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.

110. The OBNA requires any notice to be provided "without any reasonable delay."

111. The OBNA indicates a state-created policy that entities acting within Oklahoma not put Oklahoma residents at risk by implementing unreasonable data security measures, including failing to encrypt personal information stored on any entity's systems. Similarly, the OBNA requires entities who experienced a breach to notify residents whose personal information was reasonably believed to have been accessed.

112. Plaintiff and the Class are within the class of individuals intended to be protected by the OBNA. The Act includes payment card information in the definition of "Personal information." § 162(6). Additionally, by requiring notice upon discovery of a breach, the Act ensures Financial Institutions can prevent fraudulent transactions from occurring, thus protecting financial institutions from additional harm caused by the data breach.

113. Sonic breached the OBNA by failing to provide reasonable notice of the breach to affected consumers. By violating the OBNA, Sonic committed negligence *per se*.

114. The Oklahoma Consumer Protection Act ("OCPA") prohibits, among other things, businesses from "[c]omit[ing] an unfair or deceptive trade practice as defined in Section 752 of this title[.]" 15 OK Stat. § 15-753.

115. The OCPA defines an "unfair trade practice" as "any practice which offends established public policy or . . . is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *Id.* at 15-752(14).

116. The OCPA further defines a "deceptive trade practice" as "a misrepresentation, omission or other practice that has deceived or could reasonably be expected to deceive or mislead a person to the detriment of that. Such a practice may occur before, during or after a consumer transaction is entered into . . . ." *Id.* at § 15-752 (13).

117. Sonic acted "unfairly" under the OCPA by deliberately neglecting to institute reasonable data security measures, foreseeably increasing the likelihood of a data breach and harm to financial institutions. While Sonic saved money be choosing not to adequately invest in its data security measures, it increased the risk of harm to the financial institutions that would be reasonable for remediating the damages of a breach, including replacing compromised cards and reimbursing consumers for fraud on their accounts attributable to the payment card information stolen from Sonic during the Data Breach. Sonic knowingly, deliberately, and unfairly placed the onus of paying to rectify its insecure data security measures on plaintiffs.

118. Sonic also acted "deceptively" by failing to inform consumers and financial institutions that it had implemented unreasonable data security measures. Sonic's practice of accepting credit and debit card payments for its goods and services represents to the public and to the financial industry that it has implemented the necessary data security measures to keep payment card information safe. Despite representing that its systems were secure, Sonic used outdate and insecure data security measures that eventually allowed hackers to breach its systems for months without notice. Sonic's actions misled consumers and the financial industry as to the state of its data security.

119. Plaintiff and the Class are within the class of individuals intended to be protected by the OBNA. The Act is intended to protect both businesses and individuals from unfair and deceptive conduct and to facilitate consumer transactions. Financial institutions, like Plaintiff and the Class, are a necessary part of establishing consumer transactions by facilitating methods of payment through checks, credit cards, debit cards, and other means.

120. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

121. Because no statutes of other states are implicated, Oklahoma common law applies to Plaintiff and the Class's negligence per se claim.

**COUNT III**
**Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §§17200, *et seq.*, Based on "Unfair" and/or "Unlawful" Acts and Practices**
**(On Behalf of Plaintiff AAFCU and the California Class)**

122. Plaintiff AAFCU incorporates and realleges each and every allegation contained above as if fully set forth herein.

123. Plaintiff AAFCU brings this claim on behalf of itself and the California Class pursuant to the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, *et seq*.

124. Plaintiff AAFCU, and Sonic are "persons" within the meaning of Cal. Bus. & Prof. Code §17201.

125. The UCL prohibits unfair competition, which includes an "unlawful, unfair or fraudulent" act or practice. Cal. Bus. & Prof. Code §17200.

126. Under the UCL, any business act or practice that is unethical, oppressive, unscrupulous, and/or substantially injurious to consumers, or that violates a legislatively declared policy, constitutes an unfair business act or practice.

127. The violation of any law constitutes an unlawful business practice under the UCL.

128. Sonic engaged in unfair and unlawful business practices prohibited by the UCL by unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data and prevent the Data Breach. These unfair and unlawful practices occurred repeatedly in connection with Sonic's trade or business.

129. Sonic's affirmative acts in adopting and maintaining inadequate data security measures are unfair within the meaning of the UCL, because they constituted immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition.

130. Sonic's implementation of inadequate data security measures also was unfair within the meaning of the UCL, because its conduct undermined California public policy that businesses protect personal and financial information as reflected in Article I, Section 1 of the California Constitution (enacted because of private sector data processing activity and stating that all people have an inalienable right to privacy) and in statutes such as the Online Privacy Protection Act, Cal. Bus. & Prof. Code §22578 (explaining that the Legislature's intent was to have a uniform policy statewide regarding privacy policies on the Internet); the Information Practices Act, Cal. Civ. Code §1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal.

Civ. Code §1798.81.5(a)(1) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); and the FTCA, 15 U.S.C. §45(a)(1), which prohibits unfair trade practices.

131. Sonic's violations of the California Customer Records Act, Cal. Civ. Code §1798.81.5(b) (the "California Customer Records Act"), moreover, constitute unlawful acts or practices under the UCL. The California Customer Records Act requires a "business that owns, licenses, or maintains personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" and "to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Sonic failed to implement and maintain such reasonable security procedures and practices before and at the time of the Data Breach. As a result, Sonic violated the California Customer Records Act, Cal. Civ. Code §1798.81.5(b).

132. Sonic's violations of the FTCA, 15 U.S.C. §45(a)(1), as alleged herein, also constitute unlawful acts or practices under the UCL.

133. Plaintiff AAFCU and the California Class reasonably expected Sonic to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

134. Sonic's conduct harmed competition. While Sonic cut corners and minimized costs, its competitors spent the time and money necessary to ensure Payment Card Data was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff AAFCU and the California Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing

its networks and protecting Payment Card Data, there is no way Plaintiff AAFCU or the California Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

135. Plaintiff AAFCU and the California Class have members located in California whose payment cards were impacted by the Data Breach. For these California-based cardholders, Plaintiff AAFCU and the California Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff AAFCU and the California Class suffered an injury in California.

136. Sonic willfully engaged in the unfair and unlawful acts and practices described above and knew or should have known that those acts and practices were unfair and unlawful in violation of the UCL.

137. As a direct and proximate result of Sonic's unfair and unlawful practices and violation of UCL, Plaintiff AAFCU and the California Class have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

**COUNT IV**
**Violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§501.201, *et seq*.**
**(On Behalf of Plaintiff AAFCU and the Florida Class)**

138. Plaintiff AAFCU, individually and on behalf of the Florida Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

139. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§501.201, et seq., prohibits unfair methods of competition, unconscionable acts or

practices, and unfair or deceptive acts or practices in the conduct of trade or commerce. See Fla. Stat. §501.204(1). The FDUTPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. See Fla. Stat. §501.204(2); see also Fla. Stat. §§501.202(3), 501.203(3)(a)-(c).

140. Plaintiff and Florida Class members are "consumers" as defined by Fla. Stat. §501.203.

141. Plaintiff and the Florida Class have members located in Florida whose payment cards were impacted by the Data Breach. For these Florida-based cardholders, Plaintiff AAFCU and the Florida Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff AAFCU and the Florida Class suffered an injury in Florida.

142. The conduct constituting Sonic's unfair acts and practices under this claim occurred primarily and substantially in Florida because Sonic's unlawful conduct: (a) foreseeably impacted financial institutions located in Florida, which is where members of the Florida Class incurred losses and suffered damages; (b) foreseeably impacted consumers residing in Florida whose Payment Card Data was compromised in the Data Breach; and (c) otherwise interfered with trade or commerce in Florida.

143. Sonic advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

144. Sonic engaged in unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of trade and commerce, in violation of Fla. Stat. §501.204(1), including:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2), which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2).

145. Sonic's conduct is not only deceptive, but unfair and unconscionable within the meaning of FDUTPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff AAFCU , to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Florida Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Florida Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

146. Sonic's conduct is also unfair or unconscionable within the meaning of FDUTPA because it undermines public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. §45, and Fla. Stat. §501.171(2).

147. Sonic's unlawful acts and practices complained of herein affect the consumer marketplace and the public interest, including the 5 million U.S. consumers, including numerous Floridians, and thousands of U.S. financial institutions, including banks and credit unions headquartered in Florida, affected by the Sonic Data Breach.

148. As a direct and proximate result of Sonic's unconscionable, unfair, and deceptive acts and practices, Plaintiff AAFCU and Florida Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

149. Plaintiff AAFCU and Florida Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. §501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. §501.2105(1); and any other relief that is just and proper.

**COUNT V**
**Violation of the Georgia Deceptive Trade Practices Act,**
**Ga. Code Ann. §§10-1-370, *et seq*.**
**(On Behalf of AAFCU and the Georgia Class)**

150. Plaintiff AAFCU, individually and on behalf of the Georgia Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

151. The Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), Ga. Code Ann. §§10-1-370, et seq., prohibits deceptive trade practices in the course of a person's "business, vocation, or occupation." Ga. Code Ann. §10-1-372(a).

152. Sonic, Plaintiff AAFCU, and Georgia Class members are "persons" within the meaning of Ga. Code Ann. §10-1-371(5).

153. Sonic engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code Ann. §10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

c. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

154. Sonic's deceptive trade practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data , which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45.

155. Sonic's conduct caused substantial injury to consumers and businesses and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff AAFCU, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Georgia Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Georgia Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

156. Sonic intended to mislead Plaintiff and Georgia Class members and induce them to rely on its misrepresentations and omissions.

157. In the course of its business, Sonic engaged in activities with a tendency or capacity to deceive.

158. As a direct and proximate result of Sonic's deceptive trade practices, Plaintiff AAFCU and Georgia Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Payment Card Data.

159. Plaintiff and Georgia Class members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under Ga. Code Ann. §10-1-373.

**COUNT VI**
**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§505/1, *et seq*.**
**(On Behalf of Plaintiff AAFCU and the Illinois Class)**

160. Plaintiff AAFCU, individually and on behalf of the Illinois Class, repeats and realleges each and every allegation as contained above as if fully alleged herein.

161. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 Ill. Comp. Stat. §§505/1, et seq., prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce. *See* 815 Ill. Comp. Stat. §505/2. ICFA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. *See id*.

162. Sonic is a "person" as defined by 815 Ill. Comp. Stat. §505/1(c).

163. Sonic's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. §505/1(f).

164. Plaintiff and Illinois Class members are "persons," as defined in 815 Ill. Comp. Stat. Ann. §505/1(c), are "consumers," as defined in 815 Ill. Comp. Stat. Ann. §5051(e), and satisfy the consumer nexus test in that Sonic's unfair and deceptive acts and practices were directed at and impacted the market generally and/or otherwise implicate consumer protection concerns where Sonic's unfair and deceptive acts and practices have impacted at least thousands of consumers in Illinois and millions nationwide and remedying Sonic's wrongdoing through the relief requested herein would serve the interests of consumers. Furthermore, Plaintiff and the Illinois Class have members located in Illinois whose payment cards were impacted by the Data Breach. For these Illinois-based cardholders, Plaintiff AAFCU and the Illinois Class reimbursed them for fraudulent

transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff AAFCU and the Illinois Class suffered an injury in Illinois.

165. Sonic advertised, offered, or sold goods or services in Illinois and therefore engaged in trade or commerce directly or indirectly affecting the people of Illinois.

166. Under ICFA, the use or employment of any practice described in Section 2 of the Uniform Deceptive Trade Practices Act ("UTPA"), 815 Ill. Comp. Stat. Ann. §510/2, in the conduct of any trade or commerce is unlawful whether any person has in fact been misled, deceived, or damaged thereby.

167. Sonic engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

c. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

168. Sonic's unfair and deceptive trade practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45and

815 Ill. Comp. Stat. §530/45, which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45 and 815 Ill. Comp. Stat. §530/45.

169. Sonic's conduct constitutes unfair methods of competition and unfair practices within the meaning of ICFA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Illinois Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Illinois Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

170. Sonic's conduct also constitutes unfair practices within the meaning of ICFA because it undermines public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. §45, and 815 Ill. Comp. Stat. §530/45.

171. Sonic intended to mislead Plaintiff and Illinois Class members and induce them to rely on its misrepresentations.

172. Plaintiff and the Illinois Class reasonably expected Sonic to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data.

173. As a direct and proximate result of Sonic's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

174. Plaintiff and Illinois Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

**COUNT VII**
**Violation of the Louisiana Unfair Trade Practices Act, La. Stat. Ann. §§51:1401, *et seq*.**
**(On Behalf of Plaintiff AAFCU and the Louisiana Class)**

175. Plaintiff AAFCU, individually and on behalf of the Louisiana Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

176. The Louisiana Unfair Trade Practices and Consumer Protection Law ("LUPTA") makes unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Stat. Ann. §51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

177. Sonic, Plaintiff, and the Louisiana Class members are "persons" within the meaning of the La. Stat. Ann. §51:1402(8).

178. Plaintiff and Louisiana Class members are "consumers" within the meaning of La. Stat. Ann. §51:1402(1). Plaintiff and the Louisiana Class are financial institutions located in Louisiana, of which there are more than 250, that extend the credit that facilitates economic growth in Louisiana and that therefore rely on the integrity of the credit reporting industry.

179. Sonic engaged in "trade" or "commerce" within the meaning of La. Stat. Ann. §51:1402(10).

180. Sonic participated in unfair and deceptive acts and practices that violated the LUTPA, including:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45 which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45.

181. Sonic's conduct is not only deceptive, but also unfair within the meaning of LUTPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to

consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Louisiana Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Louisiana Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

182. Sonic's conduct is also unfair within the meaning of LUTPA because it undermines Louisiana public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. §45,.

183. Sonic intended to mislead Plaintiff and Louisiana Class members and induce them to rely on its misrepresentations.

184. As a direct and proximate result of Sonic's unfair and deceptive acts and practices, Plaintiff and Louisiana Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

185. Plaintiff and Louisiana Class members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Sonic's knowing

violations of the LUTPA; declaratory relief; attorneys' fees; and any other relief that is just and proper.

**COUNT VIII**
**Violation of the Massachusetts Consumer Protection Act, Mass. Gen. Laws Ann. Ch. 93A, §§1, *et seq*.**
**(On Behalf of Plaintiff AAFCU and the Massachusetts Class)**

186. Plaintiff AAFCU, individually and on behalf of the Massachusetts Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

187. The Massachusetts Consumer Protection Act, Mass. Gen. Laws, Ch. 93A, et seq. ("Chapter 93A"), makes it unlawful to engage in any "unfair or deceptive acts or practices in the conduct of any trade or commerce" and, in interpreting its provisions, requires consideration be given to interpretations by the FTC relating to Section 5 of the FTCA. *See* Mass. Gen. Laws, Ch. 93A §§2(a) and (b).

188. Sonic, Plaintiff, and Massachusetts Class members are "persons" as meant by Mass. Gen. Laws, Ch. 93A, §1(a).

189. Plaintiff and the Massachusetts Class have members located in Massachusetts. The Massachusetts Class consists of more than 250 financial institutions that extend the credit that facilitates economic growth in Massachusetts. The conduct constituting Sonic's unfair acts and practices under this claim occurred primarily and substantially in Massachusetts under the pragmatic, functional analysis employed by courts because Sonic's unlawful conduct: (a) foreseeably impacted financial institutions located in Massachusetts, which is where members of the Massachusetts Class incurred losses and suffered damages; (b) foreseeably impacted consumers residing in Massachusetts whose

Payment Card Data was compromised in the Data Breach; and (c) otherwise interfered with trade or commerce in Massachusetts.

190. Sonic, as well as Plaintiff and the Massachusetts Class, operate in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, §1(b).

191. Sonic advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, §1(b).

192. Sonic engaged in unfair methods of competition and unfair or deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, §§2(a) and 11, including:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, §2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45 and the Massachusetts

Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, §2; 201 Mass. Code Regs. 17.01-05.

193. Sonic's conduct is unfair within the meaning of Chapter 93A because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Massachusetts Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Massachusetts Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

194. Sonic's conduct also was unfair within the meaning of Chapter 93A because it undermines public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. §45 and Mass. Gen. Laws, Ch. 93H, §2 and 201 CMR 17.01-05.

195. Sonic intended to mislead Plaintiff and Massachusetts Class members and induce them to rely on its misrepresentations.

196. As a direct and proximate result of Sonic's unfair and deceptive acts and practices, Plaintiff and Massachusetts Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary

damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

197. Plaintiff and Massachusetts Class members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

**COUNT IX**
**Violation of the Minnesota Plastic Card Security Act, Minn. Stat. §325E.64**
**(On Behalf of Plaintiff AAFCU and the Minnesota Class)**

198. Plaintiff AAFCU, individually and on behalf of the Minnesota Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

199. The Minnesota Plastic Card Security Act, Minn. Stat. §325E.64, imposes a duty on merchants conducting business in Minnesota to safeguard payment card data obtained from their customers by deleting such data immediately after authorization of a credit card transaction or, in the case of a PIN debit transaction, within 48 hours after authorization of the transaction. A private right of action is expressly provided to those injured by a violation of the statute.

200. Specifically, Minn. Stat. §325E.64, subdivision 2 provides:

> No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

201. Sonic conducts business in Minnesota.

202. Sonic regularly accepts debit and credit cards, which are "access devices" within the meaning of the statute, in connection with sales transactions and for the purpose of conducting business in Minnesota.

203. Sonic violated the Minnesota Plastic Card Security Act by retaining payment card data (the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data) longer than allowed by the statute – *i.e.*, subsequent to the authorization of the transaction or, in the case of a PIN debit transaction, subsequent to 48 hours after authorization.

204. Plaintiff issues payment cards and received fraud alerts from one or more of the payment card brands identifying payment cards it issued that were compromised in the Sonic Data Breach.

205. As a direct and proximate result of Sonic's violation of the Minnesota Plastic Card Security Act, Plaintiff and members of the Minnesota Class that issued payment cards with Payment Card Data compromised in the Data Breach have suffered and will continue to suffer damage, including the costs specifically set forth in Minn. Stat. §325E.64, and thus are entitled to damages in an amount to be proven at trial.

**COUNT X**
**Violation of Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§ 598.0903, *et seq.***
**(On Behalf of Plaintiff AAFCU and the Nevada Class)**

206. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

207. The Nevada Deceptive Trade Practices Act ("NDTPA"), Nev. Rev. Stat. §§ 598.0903, *et seq.*, prohibits deceptive trade practices in the course of a person's "business or occupation." Nev. Rev. Stat. § 598.0915.

208. Nev. Rev. Stat. § 41.600(1) provides that "[a]n action may be brought by any person who is a victim of consumer fraud."

209. "Consumer fraud" is defined as, *inter alia*, "a deceptive trade practice as defined in Nev. Rev. Stat. §§ 598.0915 to 598.0925, inclusive." Nev. Rev. Stat. § 41.600(2)(e).

210. Business competitors are included in the definition of "victims" for purposes of consumer fraud claims. *See* Nev. Rev. Stat. § 598.0953(1); *S. Serv. Corp. v. Excel Bldg. Servs., Inc.*, 617 F. Supp. 2d 1097, 1100 (D. Nev. 2007) (concluding that Nevada law allows a competitor to sue under the consumer fraud statutes when that competitor can demonstrate it was directly harmed by the defendant's deceptive trade practices).

211. Sonic engaged in deceptive trade practices in the course of its business in violation of Nev. Rev. Stat. § 598.0915, including:

a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations or quantities of goods or services for sale or lease or a false representation as to the sponsorship, approval, status, affiliation or connection of a person therewith;

b. Representing that goods or services for sale or lease are of a particular standard, quality or grade, or that such goods are of a particular style or model, if he or she knowns or should know that they are of another standard, quality, grade, style or model; and

c. Advertises goods or services with intent not to sell or lease them as advertised.

212. Sonic engaged in deceptive trade practices in the course of its business in violation of Nev. Rev. Stat. § 598.0923(A), including:

a. Failing to disclose a material fact in connection with the sale or lease of goods or services; and

b. Violating a state or federal statute or regulation relating to the sale or lease of goods or services.

213. Sonic's deceptive trade practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. § 45.

214. Sonic's conduct caused substantial injury to consumers and businesses and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff AAFCU, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Nevada Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Nevada Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

215. Sonic intended to mislead Plaintiff and the Nevada Class members and induce them to rely on its misrepresentations.

216. As a direct and proximate result of Sonic's deceptive trade practices, Plaintiff and the Nevada Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased imminent risk of fraud and identity theft.

217. Plaintiff and the Nevada class members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

**COUNT XI**
**Violation of New Hampshire Consumer Protection Act, N.H. Stat. §§358-A:1, *et seq.***
**(On Behalf of Plaintiff AAFCU and the New Hampshire Class)**

218. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

219. Plaintiff and the New Hampshire Class are "persons" within the meaning of N.H. Rev. Stat. §358-A:1(I).

220. Defendant is engaged in "trade" and "commerce" within the meaning of N.H. Rev. Stat. §358-A:1(II).

221. The New Hampshire Consumer Protection Act ("NHCPA") prohibits unfair acts or practices in the conduct of trade or commerce. An unfair practice is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers, offends public policy as established by law or by other established concepts of unfairness, and is of the type proscribed by the NHCPA, attaining the level of rascality that would raise an eyebrow of someone inured to the rough and tumble of the world of commerce. In interpreting its provisions, the NHCPA requires express consideration be given to interpretations by the FTC relating to Section 5 of the FTCA. See N.H. Rev. Stat. §358-A:13.

222. Sonic engaged in unfair business practices prohibited by the NHCPA by unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data and prevent the Data Breach. These unfair practices occurred repeatedly in connection with Sonic's trade or business.

223. Sonic's affirmative acts in adopting and maintaining inadequate security measures are unfair within the meaning of the NHCPA because they constituted immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition.

224. Sonic's failure also was unfair within the meaning of NHCPA because its conduct undermined New Hampshire public policy that personal and financial information be protected from disclosure, as reflected in N.H. Rev. Stat. §359-C:2.

225. Sonic's misconduct, as alleged herein, is of the type proscribed by the NHCPA, attaining the level of rascality that would raise an eyebrow of someone inured to the rough and tumble of the world of commerce, because the consequences of Sonic's inadequate data security measures were entirely foreseeable, yet Sonic chose to not implement even those most basic data security measures. By accepting payment cards, Sonic represented to the public and to Plaintiffs and the Class that it would safeguard Payment Card Data. By knowingly implementing inadequate data security measures, Sonic created a likelihood of confusion because the public, Plaintiffs, and the Class had no way of ascertaining the adequacy of Sonic's data security measures.

226. Plaintiff and the New Hampshire Class reasonably expected Sonic to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect Payment Card Data, which contains their cardholders' personal and financial information.

227. Sonic's conduct harmed competition. While Sonic cut corners and minimized costs, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff and the New Hampshire Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the New Hampshire Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

228. Plaintiff and the New Hampshire Class have members located in New Hampshire whose payment cards were impacted by the Data Breach. For these New Hampshire-based cardholders, Plaintiff and the New Hampshire Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff and the New Hampshire Class suffered an injury in New Hampshire.

229. Sonic willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of the NHCPA.

230. As a direct and proximate result of Sonic's unfair practices and violation of the NHCPA, Plaintiff and the New Hampshire Class have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

**COUNT XII**

**Violation of the New Mexico Unfair Practices Act, N.M. Stat. Ann. §§57-12-1, *et seq*. (On Behalf of Plaintiff AAFCU and the New Mexico Class)**

231. Plaintiff AAFCU, individually and on behalf of the New Mexico Class, repeats and realleges each and every allegation contained as if fully alleged herein.

232. The New Mexico Unfair Practices Act ("NMUPA") N.M. Stat. Ann. §§57-12-1, *et seq.*, prohibits unfair or deceptive trade practices in the conduct of any trade or commerce. *See* N.M. Stat. Ann. §57-12-3; *see also* N.M. Stat. Ann. §57-12-2(D). The NMUPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. N.M. Stat. Ann. §57-12-4.

233. Sonic is a "person" as meant by N.M. Stat. Ann. §57-12-2(A).

234. Plaintiff and members of the New Mexico Class are "persons" as meant by N.M. Stat. Ann. §57-12-2(A). Plaintiff and the New Mexico Class have members located in New Mexico. The New Mexico Class is comprised of financial institutions located in New Mexico, of which there are more than 50 that extend the credit that facilitates economic growth in New Mexico.

235. Sonic was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. §57-12-2(C) when engaging in the conduct alleged, directly or indirectly affecting the people of New Mexico.

236. Sonic engaged in unfair and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following:

a. Knowingly representing that its goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. §57-12-2(D)(5); and

b. Knowingly representing that its goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. §57-12-2(D)(7).

237. Sonic's unfair and deceptive acts and practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

238. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

239. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, and N.M. Stat. Ann. §57-12B-3(D), and mandating reasonable data security, N.M. Stat. Ann. §57-12C-4, which was a direct and proximate cause of the Sonic Data Breach;

240. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

241. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, and mandating reasonable data security, N.M. Stat. Ann. §57-12C-4.

242. Sonic's conduct is unfair within the meaning of NMUPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and

the New Mexico Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the New Mexico Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests other than its conduct responsible for the Data Breach.

243. Sonic's conduct is also unfair and unconscionable within the meaning of NMUPA because it undermines public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. §45, and New Mexico statutes mandating reasonable data security, N.M. Stat. Ann. §57-12C-4.

244. Sonic intended to mislead Plaintiff and New Mexico Class members and induce them to rely on its misrepresentations.

245. As a direct and proximate result of Sonic's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

246. Plaintiff and New Mexico Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

**COUNT XIII**
**Violation of New York General Business Law, N.Y. Gen. Bus. Law §§349, *et seq.***
**(On Behalf of Plaintiff AAFCU and the New York Class)**

247. Plaintiff AAFCU, individually and on behalf of the New York Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

248. New York General Business Law §349 ("GBL §349") prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. Plaintiff and the New York Class have members located in New York. The New York Class is comprised of financial institutions located in New York, of which there are more than 400, which extend the credit that facilitates economic growth in New York.

249. Sonic engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of GBL §349, including:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed in the FTCA, 15 U.S.C. §45, which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data including duties imposed in the FTCA, 15 U.S.C. §45.

250. Sonic's conduct caused substantial injury to consumers and businesses and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card

Data. Further, the injuries suffered by Plaintiff and the New York Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the New York Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

251. Sonic's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the thousands of New Yorkers affected by the Sonic Data Breach. Sonic's unlawful acts and practices complained of herein affect consumers at large and the public interest, including the thousands of New Yorkers and banks and credit unions headquartered in New York affected by the Sonic Data Breach. Sonic's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiff and Class members, regarding the security and accuracy of the Payment Card Data it obtains, stores, uses, transmits, and manages. Sonic's violations present a continuing risk to Plaintiff and Class members, as well as to the general public.

252. Therefore, Plaintiff brings this action on behalf of itself and Class members for the public benefit in order to promote the public interests in the provision of truthful, fair information that enables financial institutions that extend credit to consumers and the public at large to make informed decisions related to the security of Payment Card Data, and to protect the public from Sonic's unlawful acts and practices.

253. As a direct and proximate result of Sonic's deceptive and unlawful acts and practices, Plaintiff and New York Class members have suffered and will continue to suffer

injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

254. Plaintiff and New York Class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

**COUNT XIV**
**Violation of the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §§75-1.1, *et seq*.**
**(On Behalf of Plaintiff AAFCU and the North Carolina Class)**

255. Plaintiff AAFCU, individually and on behalf of the North Carolina Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

256. The North Carolina Unfair and Deceptive Trade Practices Act ("NCUDTPA") prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." N.C. Gen. Stat. §75-1.1.

257. Sonic advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. §75-1.1(b).

258. Sonic engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. §75-1.1, including:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45.

259. Sonic's conduct constitutes unfair methods of competition and unfair practices within the meaning of NCUDTPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the North Carolina Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the North Carolina Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

260. Sonic's conduct also constitutes unfair practices within the meaning of NCUDTPA, because it undermines public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. §45.

261. Sonic intended to mislead Plaintiff and North Carolina Class members and induce them to rely on its misrepresentations.

262. As a direct and proximate result of Sonic's unfair and deceptive acts and practices, Plaintiff and North Carolina Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

263. Sonic's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitutes a separate offense pursuant to N.C. Gen. Stat. §75-8.

264. Plaintiff and North Carolina Class members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

**COUNT XV**
**Violation of the Ohio Deceptive Trade Practices Act, Ohio Rev. Code Ann. Ann. §§4165.01, *et seq.***
**(On Behalf of Plaintiff AAFCU and the Ohio Class)**

265. Plaintiff AAFCU, individually and on behalf of the Ohio Class, repeats and realleges each and every allegation above as if fully alleged herein.

266. The Ohio Deceptive Trade Practices Act ("ODTPA"), Ohio Rev. Code Ann. §§4165.01, *et seq.*, prohibits deceptive trade practices in the course of a person's "business, vocation, or occupation." Ohio Rev. Code Ann. §4165.02(A).

267. Sonic, Plaintiff, and Ohio Class members are "persons," as defined by Ohio Rev. Code Ann. §4165.01(D).

268. Plaintiff and the Ohio Class have members located in Ohio. The Ohio Class is comprised of more than 100 financial institutions that extend the credit that facilitates economic growth in Ohio.

269. Sonic advertised, offered, or sold goods or services in Ohio and engaged in business directly or indirectly affecting the people of Ohio.

270. Sonic engaged in deceptive trade practices in the course of its business, in violation of Ohio Rev. Code Ann. §4165.02, including:

a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code Ann. §4165.02(A)(7); and

b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code Ann. §4165.02(A)(9).

271. Sonic's deceptive trade practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

272. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

273. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, which was a direct and proximate cause of the Sonic Data Breach;

274. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

275. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45.

276. Sonic's conduct caused substantial injury to consumers and businesses and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Ohio Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Ohio Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

277. Sonic intended to mislead Plaintiff and Ohio Class members and induce them to rely on its misrepresentations.

278. As a direct and proximate result of Sonic's deceptive trade practices, Plaintiff and Ohio Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

279. Plaintiff and Ohio Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

**COUNT XVI**
**Violation of the South Dakota Deceptive Trade Practices and Consumer Protection Act, SDCL § 37-24-1, *et seq.***
**(On Behalf of Plaintiff AAFCU and the South Dakota Class)**

280. Plaintiff AAFCU, individually and on behalf of the South Dakota Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

281. The South Dakota Deceptive Trade Practices and Consumer Protection Act ("SDDTPCPA"), SDCL § 37-24-1, et seq., prohibits "deceptive act[s] or practice[s], fraud, false promises, or misrepresentations . . . in connection with the sale or advertisement of any merchandise." SDCL § 37-24-6(1).

282. Sonic, Plaintiff AAFCU, and the South Dakota class members are "persons" as defined by SDCL § 37-24-1(8).

283. Sonic's conduct as described herein was in the conduct of "trade" or "commerce" as defined by SDCL § 37-24-1(13).

284. Sonic advertised, offered, or sold goods or services in South Dakota and therefore engaged in trade or commerce directly or indirectly affecting the people of South Dakota.

285. Sonic engaged in deceptive trade practices in the conduct of its business in violation of SDCL § 37-24-6, including knowingly acting, using, or employing a deceptive act or practice, fraud, false pretense, false promise, or misrepresentation in connection with the sale or advertisement of merchandise.

286. Sonic's deceptive trade practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Sonic Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Sonic Data Breach;

d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. § 45.

287. Sonic's conduct constitutes unfair methods of competition and unfair practices within the meaning of SDDTPCPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the South Dakota Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the South Dakota Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

288. Sonic's conduct also constitutes unfair practices within the meaning of SDDTPCPA, because it undermines public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. § 45.

289. Sonic intended to mislead Plaintiff and the South Dakota Class members and induce them to rely upon its misrepresentations.

290. As a direct and proximate result of Sonic's unfair and deceptive acts and practices, Plaintiff and the South Dakota Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

291. Plaintiff and the South Dakota Class members seek all monetary and non-monetary relief allowed by law, including actual damages, attorneys' fees, and costs.

**COUNT XVII**
**Violation of the Tennessee Consumer Protection Act, Tenn. Code Ann. §§47-18-101, *et seq*.**
**(On Behalf of Plaintiff AAFCU and the Tennessee Class)**

292. Plaintiff AAFCU, individually and on behalf of the Tennessee Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

293. The Tennessee Consumer Protection Act ("TCPA") prohibits "unfair or deceptive acts or practices affecting the conduct of any trade or commerce[.]" Tenn. Code Ann. §47-18-104(b). The TCPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. Tenn. Code Ann. §47-18-115.

294. Sonic is a "person," as defined by Tenn. Code Ann. §47-18-103(13).

295. Plaintiff and Tennessee Class members are "persons," as defined by Tenn. Code Ann. §47-18-103(13), and "consumers," as meant by Tenn. Code Ann. §47-18-103(2). Plaintiff and the Tennessee Class have members located in Tennessee. The Tennessee Class is comprised of more than 250 financial institutions that extend the credit that facilitates economic growth in Tennessee.

296. Sonic advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code Ann. §§47-18-103(7), (18) & (19). Moreover, Sonic's acts or practices affected the conduct of trade or commerce, under Tenn. Code Ann. §47-18-104.

297. Sonic engaged in the following deceptive trade practices defined in Tenn. Code Ann. §47-18-104(b):

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have; and

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another. Tenn. Code Ann. §§47-18-104(b)(5) and (7).

298. Sonic's unfair and deceptive acts and practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data which was a direct and proximate cause of the Sonic Data Breach;

299. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Sonic Data Breach;

300. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45 which was a direct and proximate cause of the Sonic Data Breach;

301. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and

302. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45.

303. Sonic's conduct is not only deceptive, but also unfair within the meaning of the TCPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Sonic cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Tennessee Class are not outweighed by any countervailing benefits to consumers or competition. And, because Sonic is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Tennessee Class could have known about Sonic's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Sonic's legitimate business interests, other than its conduct responsible for the Data Breach.

304. Sonic's conduct is also unconscionable within the meaning of TCPA because it undermines Tennessee public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. §45.

305. Sonic intended to mislead Plaintiff and Tennessee Class members and induce them to rely on its misrepresentations.

306. As a direct and proximate result of Sonic's unfair and deceptive acts or practices, Plaintiff and Tennessee Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary

damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

307. Sonic's violations present a continuing risk to Plaintiff and Tennessee Class members as well as to the general public.

308. Plaintiff and Tennessee Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

**COUNT XVIII**
**Violation of the Washington Data Breach Notification Act, RCW 19.255.020**
**(On Behalf of Plaintiff AAFCU and the Washington Class)**

309. Plaintiff incorporates and re-alleges each allegation contained above as if fully set forth herein.

310. Plaintiff, individually and on behalf of the Washington Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

311. The Washington Legislature, to combat cybercrime and to protect financial institutions from negligent practices of retailers, enacted RCW 19.255.020, which states in pertinent part:

> If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach.

312. Plaintiff and Washington Class members are "financial institutions" within the meaning of RCW 19.255.020.

313. Defendant is a "business" within the meaning of RCW 19.255.020.

314. The information compromised in the Sonic Data Breach was "account information" within the meaning of RCW 19.255.020.

315. Defendant failed to take reasonable care to guard against unauthorized access to account information by, inter alia, failing to comply with the standards put forth by the PCI DSS, which standards Defendant must abide by to exercise reasonable care.

316. Such failure to take reasonable care on the part of Defendant led to Plaintiff and Washington Class members to incur costs associated with mitigating against fraud affecting their customers, arising from Defendant's wrongful acts.

317. Under RCW 19.255.020, Plaintiff and Washington Class members are entitled to reasonable actual costs related to the reissuance of credit cards and debit cards incurred to mitigate potential current or future damages to credit card and debit card holders.

**COUNT XIX**
**Violation of the Washington Consumer Protection Act, RCW Ch. 19.86, et seq.**
**On Behalf of Plaintiff AAFCU and the Washington Class)**

318. Plaintiff incorporates and re-alleges each allegation contained above as if fully set forth herein.

319. Washington's Consumer Protection Act, RCW Ch. 19.86 ("CPA"), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

320. To achieve that goal, the CPA prohibits any person from using "unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce[.]" RCW 19.86.020.

321. As alleged herein, Sonic's policies and practices relating to its sub-standard security measures for the use and retention of its customers' financial information violate the CPA because they are both unfair and deceptive.

322. Sonic had statutory, regulatory, and common law obligations to prevent the foreseeable risk of harm to others, including the Plaintiff and the Washington Class. It was foreseeable that the failure to use reasonable measures to protect Payment Card Data and to provide timely notice that a breach was detected if reasonable security measures were not taken, put consumers, Plaintiff, and members of the Washington Class at a serious risk of injury from the theft and fraudulent use of consumers' Payment Card Data. Moreover, it was foreseeable that, as a result of the theft and fraudulent use of Payment Card Data, financial institutions would be required to mitigate the fraud by canceling and reissuing the compromised cards, reimbursing their customers for fraud losses, and that the resulting financial losses would be immense.

323. Specifically, Sonic engaged in unfair acts and practices in violation of the CPA by failing to implement and maintain reasonable security measures to protect Payment Card Data, including failing to take proper precautionary measures with its payment card processing machines, failing to implement EMV chip readers, failing to comply with industry standards, and failing to comply with the PCI DSS.

324. Sonic's failure to implement and maintain reasonable security measures to protect consumers' financial information and failure to comply with industry standards and the PCI DSS were likely to, and did, cause substantial injury to consumers, Plaintiff and

the Washington Class. Sonic's acts or practice of maintaining inadequate security measures and failure to comply with industry standards and PCI DSS provided no countervailing benefit to consumers or competition.

325. As Sonic was solely responsible for securing its customer data, there is and was no way for Plaintiff and the Washington Class to know about Sonic's inadequate security practices or to avoid their injuries.

326. Further, Sonic's failure to inform Plaintiff and the Washington Class of its inadequate security practices and failure to comply with PCI DSS and industry standards, constitute deceptive acts and practices in violation of the CPA. By facilitating purchases in Sonic restaurants, Plaintiff and Washington Class members reasonably believed that Sonic would follow the required PCI DSS and industry standards and implement reasonable practices and policies for the use, retention, and security of its customers' financial information to protect against the foreseeable threat of data theft and the resulting harm. In light of the foreseeable risk of harm to consumers, Plaintiff and members of the Washington Class reasonably believed Sonic would use reasonable practices to protect Payment Card Data and comply with industry standards and PCI DSS. Sonic's acts, omissions, or practices were likely to mislead Plaintiff and members of the Washington Class.

327. Similarly, Sonic violated and continues to violate the CPA by failing to put a reasonable notification policy in place, where customers' financial information is compromised as a result of a data breach. The failure to notify consumers of the data breach was likely to cause additional harm to consumers, Plaintiff, and members of the Washington Class as it allowed the theft of additional data to continue unabated, and thereby exacerbated the injuries suffered by Plaintiff and the Washington Class. Sonic's

duty to notify consumers, Plaintiff, and the Washington Class in a reasonable manner is not outweighed by any countervailing benefits to consumers or competition.

328. Sonic's unfair acts or practices occurred in its trade or business and have injured a substantial portion of the public. Sonic's acts, practices, or omissions are injurious to the public interest as they caused injury to, and had and have the capacity to cause injury to, Plaintiff and other financial institutions, and have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of its misconduct may last for years.

329. As a direct and proximate result of Sonic's violations of the CPA prohibiting unfair and deceptive acts and practices, Plaintiff and members of the Washington Class have suffered monetary damages for which Sonic is liable.

330. Plaintiff and the Washington Class seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the CPA.

331. As redress for Sonic's repeated and ongoing violations, Plaintiff and the Washington Class are entitled to, *inter alia*, actual damages, exemplary damages, attorneys' fees, and injunctive relief.

**COUNT XX**
**Declaratory and Injunctive Relief**

332. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

333. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

334. An actual controversy has arisen in the wake of the data breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the payment card data of Plaintiff and the Class. Plaintiff alleges Sonic's actions (and inaction) in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury as additional fraud and other illegal charges are being made on payment cards Plaintiff and the Class issued.

335. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

336. Sonic owes a legal duty to secure and the sensitive financial information to which it is entrusted– specifically including information pertaining to credit and debit cards used by persons who make purchases at Sonic restaurants – and to notify financial institutions of a data breach under the common law, Section 5 of the FTCA, the OBNA, the OCPA, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

337. Sonic continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

338. Sonic's breach of its legal duty continues to cause Plaintiff harm.

339. The Court should also issue corresponding injunctive relief requiring Sonic to employ adequate security protocols consistent with industry standards to protect its customers' personal and financial information.

340. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Sonic's data systems. If another breach of Sonic's data systems occurs, Plaintiff will not have an adequate remedy

at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff for out-of-pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff, which include monetary damages that are not legally quantifiable or provable, and reputational damage.

341. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Sonic if an injunction is issued. Among other things, if Sonic suffers another massive data breach, Plaintiff and the members of the Class will likely incur millions of dollars in damage. On the other hand, the cost to Sonic of complying with an injunction by employing reasonable data security measures is relatively minimal and Sonic has a pre-existing legal obligation to employ such measures.

342. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

**PRAYER FOR RELIEF**

343. Wherefore, Plaintiff, on behalf of itself and other members of the Class, requests that this Court award relief against Sonic as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and its counsel as Class Counsel;

b. Awarding Plaintiff and the proposed Class members damages with pre-judgment and post-judgment interest;

c. Enter a declaratory judgment in favor of Plaintiff and the Class;

d. Grant Plaintiff and the Class the injunctive relief;

e. Award attorneys' fees and costs as allowed by law; and

f. Award such other and further relief as the Court may deem necessary or appropriate.

**JURY TRIAL DEMANDED**

344. Plaintiff hereby demands a jury trial for all of the claims so triable.

Respectfully submitted,

*/s/ David B. Donchin*

David B. Donchin, OBA #10783
**DURBIN LARIMORE & BIALICK**
920 North Harvey Avenue
Oklahoma City, OK 73102
Phone: 405/235-9584; Fax: 405/235-0551
ddonchin@dlb.net

Charles H. Van Horn, GA Bar No. 724710
Katherine M. Silverman, GA Bar No. 395741
**BERMAN FINK VAN HORN P.C.**
3475 Piedmont Road, NE
Suite 1100
Atlanta, GA 30305
Phone: 404/261-7711; Fax: 404/233-1943

Arthur M. Murray
Stephen B. Murray, Sr.
Caroline Thomas White
**MURRAY LAW FIRM**
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Phone: 504/525-8100; Fax: 504/584-5249
amurray@murray-lawfirm.com
smurray@murray-lawfirm.com
cthomas@murray-lawfirm.com

Brian C. Gudmundson, MN Bar No. 336695
Michael J. Laird, MN Bar No. 398436
Bryce D. Riddle, MN Bar No. 398019
**ZIMMERMAN REED LLP**
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Phone: 612/341-0400; Fax: 612/341-0844
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
bryce.riddle@zimmreed.com

Joseph P. Guglielmo
Erin Green Comite
**SCOTT+SCOTT**
**ATTORNEYS AT LAW LLP**
230 Park Avenue, 17th Floor
New York, NY 10169
Phone: 212/223-6444; Fax: 212/223-6334
jguglielmo@scott-scott.com
ecomite@scott-scott.com